ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

EDASVIC: ENABLING EFFICIENT AND DYNAMIC STORAGE VERIFICATION FOR CLOUDS OF INDUSTRIAL INTERNET PLATFORMS

Dr. M. V. NARAYANA[1], THIPPANI SWETHA[2], VAKITI SHIREESHA[3], GOTTAMUKKULA SHIVAKUMAR[4], MOTAPALUKULA SAI TEJA[5]

[1]Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Industrial Internet platforms (IIP) can provide many intelligent services based on the industrial big data stored in clouds. However, the vulnerability of cloud storage can cause data corruption, demanding verifying its integrity. Unfortunately, existing cloud storage verification approaches cannot be directly applied to IIP, since they pose heavy computational burdens on the edge side. In this work, we propose an efficient and dynamic storage verification scheme Edasvic for cloud storage in the IIP. We adopt the polynomial commitment to build an efficient homomorphic authenticator, and further design an authenticator accumulator, which can be efficiently generated with limited computational overheads. In addition, we integrate the dynamic information into the authenticator accumulator to support data dynamics. The security of Edasvic is analyzed under the random oracle model. We conduct extensive experiments to evaluate the performance of Edasvic and compare it with the state-of-the-art approaches. Experimental results affirm that Edasvic is superior to existing solutions in terms of computational efficiency.

Index Terms – Industrial Internet of Things (IIoT), Cloud Storage Verification, Dynamic Data Integrity, Provable Data Possession

(PDP), Remote Data Auditing, Secure Cloud Storage, Data Integrity Verification, Industrial Internet Platforms, Cryptographic Verification, Cloud Computing Security, Efficient Storage Management, Trusted Data Outsourcing.

I. INTRODUCTION

INDUSTRIAL Internet platforms (IIP), also called industrial IoT (IIoT) platforms (e.g., GE Predix, Siemens Mind- Sphere, PTC ThingWorx, etc.), are rapidly emerging worldwide and have received extensive attention from both academia and industry. The IIP integrates a variety of manufacturing resources or capabilities of different enterprises to provide services for platform users. Conversely, the IIP can also analyse the data from connected products, plants and systems to improve the reliability, flexibility, and efficiency of the industrial systems in different sectors, such as manufacturing, energy, logistics, etc. Existing notable IIPs including Mind Sphere and Predix are built based on an edge-cloud infrastructure in which fog nodes collect an enormous amount of industrial data from IIoT devices whilst the cloud stores these data for further optimizing operations, creating better quality products, or deploying new business models, etc. In this infrastructure, the cloud service plays an essential role in the IIP that stores all collected data for data analysis. However, it also brings security challenges to the industrial data and system. On one hand, as a centralized infrastructure, cloud storage suffers from a single point of failure due to many uncertainties, e.g., system breakdowns, power outages, etc. This gives rise to a growing number of data loss cases in many notable cloud service providers such as Google and Tencent.

II. RELATED WORK

A. Blockchain enabled fair, accountable and secure data sharing for industrial IOT

Industrial Internet of Things (IIoT) opens up a challenging research area towards improving secure data sharing which currently has several limitations. Primarily, the lack of inbuilt guarantees of honest behavior of participating, such as end-users or cloud behaving maliciously may result in disputes. Given such challenges, we propose a fair, accountable, and secure data sharing scheme, Fairshare for IIoT. In this scheme, data collected from IoT devices are processed and stored in cloud servers with intermediate fog nodes facilitating computation. Authorized clients can access this data against some fee to make strategic decisions

for improving the operational services of the IIoT system. By enabling blockchain, Fairshare prevents fraudulent activities and thereby achieves fairness such that each party gets their rightful outcome in terms of data or penalty/rewards while simultaneously ensuring accountability of the services provided by the parties. Additionally, smart contracts are designed to act as a mediator during any dispute by enforcing payment settlement. Further, security and privacy of data are ensured by suitably applying cryptographic techniques like proxy re-encryption. We prove Fairshare to be secure as long as at least one of the parties is honest. We validate Fairshare with a theoretical overhead analysis. We also build a prototype in Ethereum to estimate performance and justify comparable results with a state-of-the-art scheme both via simulation and a realistic testbed setup. We observe an additional communication overhead of 256 bytes and a cost of deployment of 1.01 USD in Ethereum which are constant irrespective of file size.

B. Trust management in industrial Internet of Things

Automobile manufacturers around the world are increasingly deploying Industrial Internet of Things (IIoT) devices in their factories to accompany the Industrial Revolution 4.0. Security and privacy are the main limitations to the integration of Internet of Things (IoT) into industrial processes. Therefore, it is necessary to protect industrial data contained in IIoT devices and keep them confidential. As a step towards this direction, in this paper, we propose a dynamic trust management model suitable for industrial environments. We propose also to change the traditional centralized architecture of IIoT networks in automotive plants into a hybrid architecture based on a set of new industrial relationship rules. The performance evaluation in this work is done in two parts. In the first part, we compare our proposed architecture with the traditional architecture of the plant's IIoT network. The results of this comparison show that our architecture is more suitable to simplify trust management of IIoT devices. In the second part, we demonstrated the ability, the adaptiveness and the resiliency of our proposed trust model against behavioral changes of IIoT nodes in malicious environments.

C. Blockchain-based offline auditing for the cloud in vehicular networks

The rapid growth of various vehicular apps such as automotive navigation and in-car entertainment has brought the explosion of vehicular data. Such a growth has given rise to a huge challenge of maintaining the quality of cloud storage services for the whole period

of storage in vehicular networks. As a result, poor quality of services easily causes data corruption problems and thereby threats vehicular data integrity. Blockchain, a tamper-proofing technique, is considered a promising approach for mitigating data integrity risks in cloud storage. However, existing blockchain-based schemes for auditing long-term cloud data integrity suffer from poor communication performance in a vehicular network. In this study, a blockchain-based offline auditing scheme for cloud storage in the vehicular network is proposed to improve auditing performance. Inspired by the data structure of blockchain, we design an evidence chain to achieve offline auditing, which allows the cloud to spontaneously generate data integrity evidence without communicating with auditors during the evidence generation phase. Furthermore, we extend our scheme to support public and automatic validation based on the smart contract. We prove the security of the proposed scheme under the random oracle model and further provide the performance evaluation by comparing with the state-of-the-art approaches.

III. PROPOSED METHODOLOGY

The proposed system introduces Edasvic, an efficient dynamic storage verification scheme that ensures the integrity of cloud-stored industrial data. It enables continuous verification without retrieving the original data, thereby reducing communication overhead and improving system efficiency. A novel authenticator accumulator is designed to combine multiple authentication values into a single compact value. This minimizes storage requirements, reduces verification time, and lowers the computational burden on edge devices and fog nodes during the auditing process. Unlike traditional cloud verification schemes, the proposed system supports dynamic data operations such as insertion, deletion, modification, and updating of data blocks. The accumulator is updated efficiently without regenerating authentication information for the entire dataset, making it suitable for real-time industrial environments The system allows a Third-Party Verifier (TPV) to verify cloud data integrity without accessing the actual contents of the stored files. The challenge-response mechanism protects data privacy while ensuring that any unauthorized modification or corruption of cloud data is detected accurately

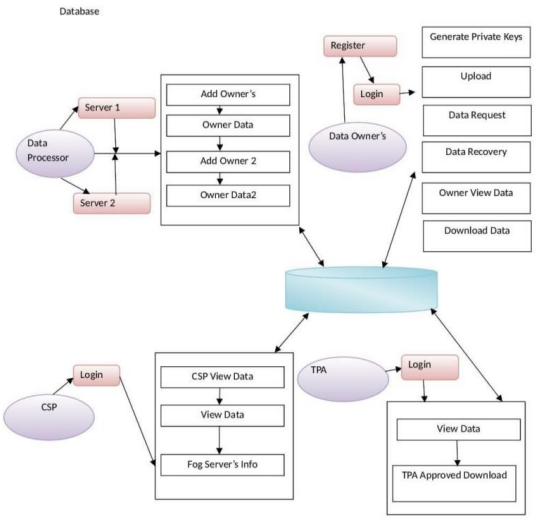
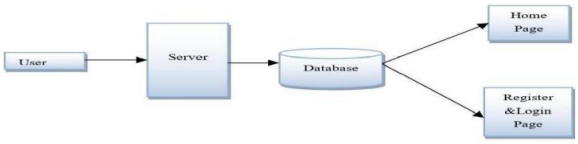


Fig. 1: System Overview

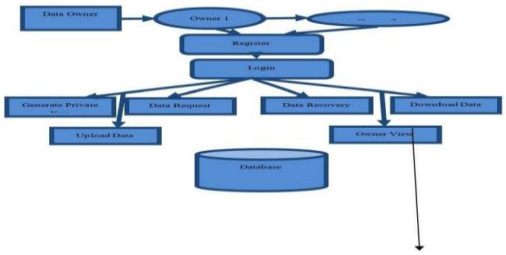
1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



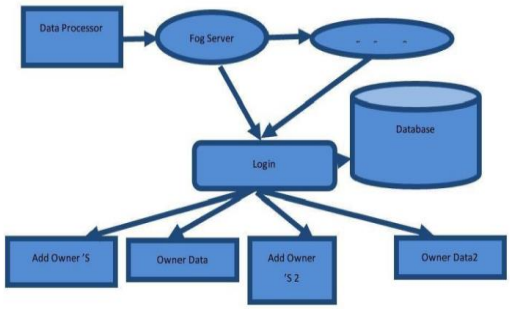
2. Owner

The Owner has a register with a user id and password. The Owner has login. It generate a private keys. The Data owner has a upload a data to store in a database. The Owner has a data request to to view a data. The Owner2 has login with a user id and password. The owner 2 has a data recovery to recover a data. The owner has a view a owner data. The data has a download a data from a database.



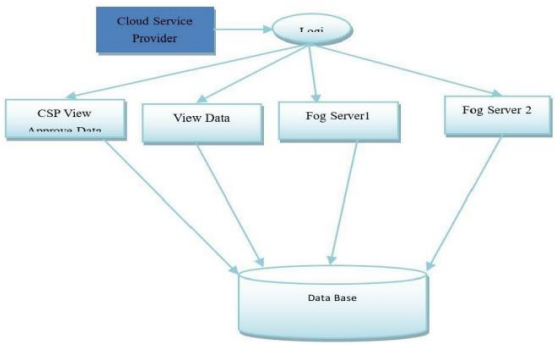
3. Data Processor

With a user ID and password, the Data Processor may be accessed. In a database, there are additional owners for fog server 1. The owner data is on the fog server 1. The login credentials for the fog server 2 are a user ID and password. To add members, the fog server2 includes an add owner2 feature. There is a fog server2 added to owner data2. Here, you divide the data into two or more sets: typically a training set and a test set. The training set is used to train the model, while the test set is used to evaluate its performance. A common ratio is 70% for training and 30% for testing, but this can vary



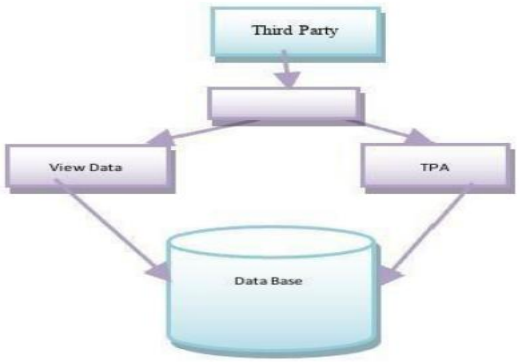
4. Cloud Service Provider

A user ID and password are required to access the cloud service provider's login. The CSP has the authority to authorize data. The CSP can see the data. The CSP displays all of the information for a fog server1. The CSP's fog server2 allows users to view all of the server information.



5.Third party Auditor

The tpa has login with a user id and password. The TPA has a view a data. The TPA has a approves a download data.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results show that the scheme performs secure integrity verification with low computational and communication costs while efficiently supporting dynamic operations such as data insertion, deletion, and modification. Compared with existing cloud storage verification methods, EDASVIC achieves faster auditing, reduced verification overhead, and improved scalability, making it suitable for secure and reliable cloud storage in Industrial Internet Platform environments.

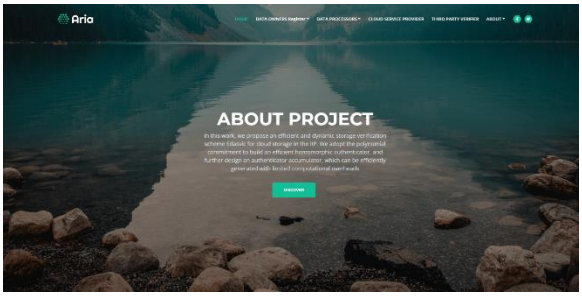


Fig. 2: Home Page

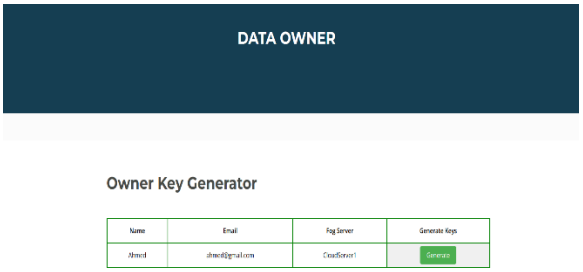


Fig. 3: Key Generator

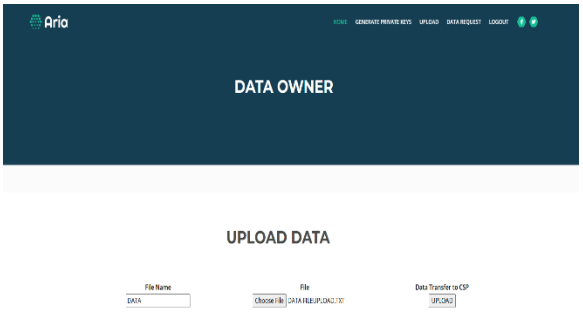


Fig. 4: Upload Data

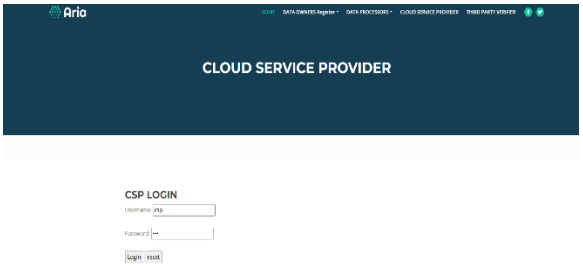


Fig. 5: CSP Login

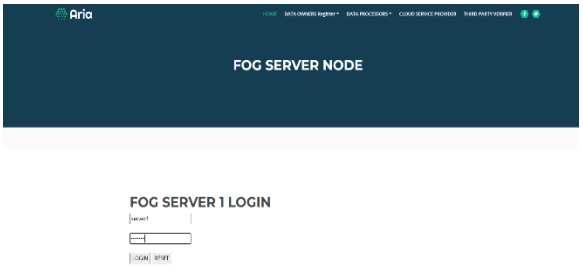


Fig. 6: Fog Server Login

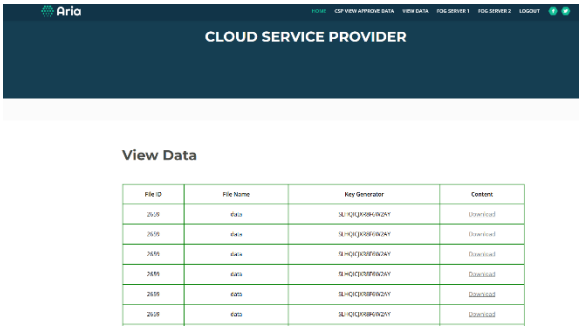


Fig. 7: View Data

V. CONCLUSION

The integrity of industrial data in the cloud can directly influence the performance of intelligent applications and services provided by industrial internet platforms, and thus should be guaranteed for both data owners and platform users. In this work, we propose an efficient and dynamic storage verification scheme for cloud-based IIP. Thanks to the design of a light-weight homomorphic authenticator and an authenticator accumulator, the computational overheads of pre-processing the data can be minimized.

REFERENCES

[1] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," J. Netw. Comput. Appl., vol. 149, Jan. 2020, Art. no. 102481.

[2] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," IEEE

Trans. Ind. Informat., vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[3] Y. Zhang and H.-Y. Wei, "Risk-aware cloud-edge computing framework for delaysensitive industrial IoTs," IEEE Trans. Netw. Service Manag., vol. 18, no. 3, pp. 2659– 2671, Sep. 2021.

[4] J. Sengupta, S. Ruj, and S. D. Bit, "FairShare: Blockchain enabled fair, accountable and secure data sharing for industrial IoT," IEEE Trans. Netw. Service Manag., vol. 20, no. 3, pp. 2929–2941, Sep. 2023.

[5] M. Aazam, S. Zeadally, and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," IEEE Commun. Mag., vol. 56, no. 5, pp. 46–52, May 2018.

[6] K. A. Nuaimi, N. Mohamed, M. A. Nuaimi, and J. Al-Jaroodi, "A survey of load balancing in cloud computing: Challenges and algorithms," in Proc. 2nd Symp. Netw. Cloud Comput. Appl., Dec. 2012, pp. 137–142.

AUTHORS Profile



Dr. M. V. Narayana received his Bachelor of Engineering (B.E.) degree in Computer Science in 2004 from JNTU Kakinada, India. He completed his Master of Technology (M.Tech) degree in Computer Science in 2010 from JNTU Hyderabad, India, and was awarded his Ph.D. in Computer Science in 2017 from JNTU Kakinada, India. With over 20 years of dedicated experience in academia and research, he currently serves as a Professor and Head of the Department (HOD) in the CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India. His research interests encompass various areas within computer science, and he has contributed significantly to the field throughout his career.



Ms. THIPPANI SWETHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. VAKITI SHIREESHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GOTTAMUKKULA SHIVAKUMAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. MOTAPALUKULA SAI TEJA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.